COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Chairman Bennie G. Thompson (D-MS)

About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II

February 6, 2020

The Committee on Homeland Security is meeting today to continue examining the Department of Homeland Security's use of facial recognition technology. The Committee held Part one of this hearing in July of last year—after news that the Department was expanding its use of facial recognition for varying purposes, such as confirming the identities of travelers, including U.S. citizens. As facial recognition technology has advanced, it has become the chosen form of biometric technology used by the government and industry. I want to reiterate that I am not wholly opposed to the use of facial recognition technology, as I recognize that it can be valuable to homeland security and serve as a facilitation tool for the Department's varying missions. But I remain deeply concerned about privacy, transparency, data security, and the accuracy of this technology and want to ensure these concerns are addressed before the Department deploys it further.

Last July, I—along with other Members of this Committee—shared these concerns at our hearing and left this room with more questions than answers. In December 2019, the National Institute for Standards and Technology (NIST) published a report that confirmed age, gender, and racial bias in some facial recognition algorithms. NIST, for example, found that depending on the algorithm, African-American and Asian-American faces were misidentified 10 to 100 times more than white faces. Although CBP touts that the match rate for its facial recognition systems is over 98 percent, it is my understanding that NIST did not test CBP's current algorithm for its December 2019 report. Moreover, CBP's figure does not account for images of travelers who could not be captured due a variety of factors such as lighting or skin tone—likely making the actual match rate significantly lower. These findings continue to suggest that some of this technology is not ready for "prime time" and requires further testing before widespread deployment.

Misidentifying even a relatively small percentage of the traveling public could affect thousands of passengers annually, and likely would have a disproportionate effect on certain individuals. This is unacceptable. Data security also remains an important concern. Last year, a CBP subcontractor experienced a significant data breach, which included traveler images being stolen. We look forward to hearing more about the lessons CBP learned from this incident and the steps that it has taken to ensure that biometric data is kept safe. Transparency continues to be key. The American people deserve to know how the Department is collecting facial recognition data, and whether the Department is in fact safeguarding their rights when deploying such technology. That is why we are here seven months later to continue our oversight.

I am pleased that we again have witnesses from CBP and NIST before us to provide us with an update and answer our questions. We will also have testimony from DHS's Office for Civil Rights and Civil Liberties. This Office is charged with ensuring the protection of our civil rights and civil liberties as it relates to the Department's activities—no easy task, especially these days. Be assured that under my leadership, this Committee will continue to hold the Department accountable for treating all Americans equitably and ensuring that our rights are protected.

# # #

Media contact: Adam Comis at (202) 225-9978